

1/22

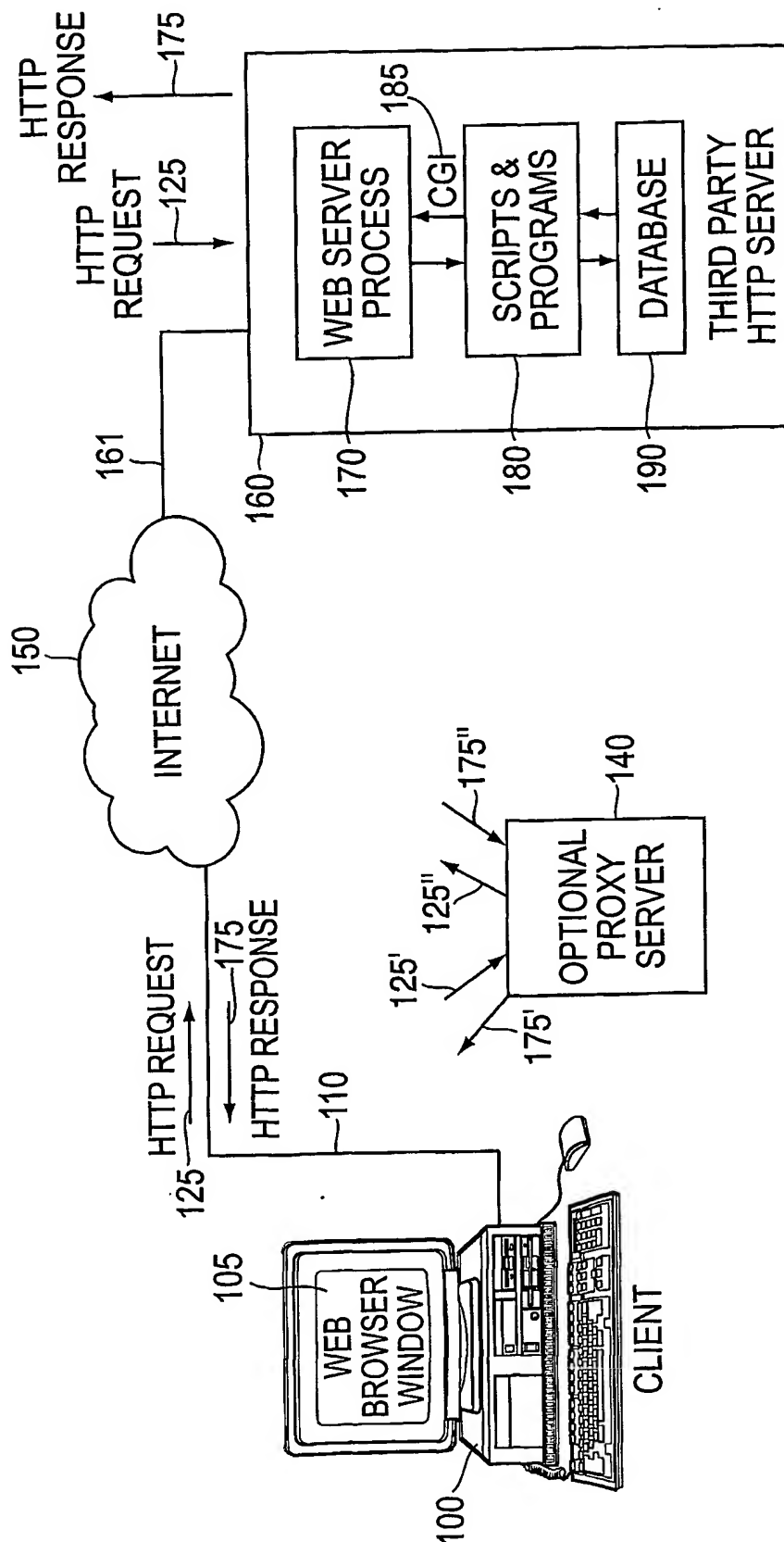


FIG. 1
PRIOR ART

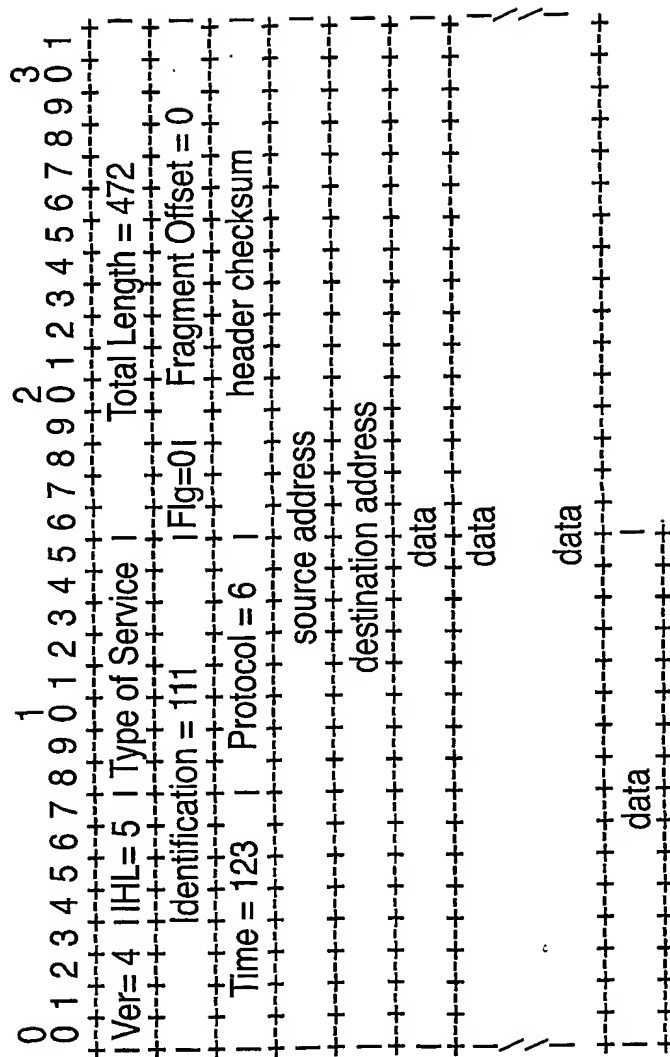


FIG. 1A
EXAMPLE INTERNET DIAGRAM

3/22

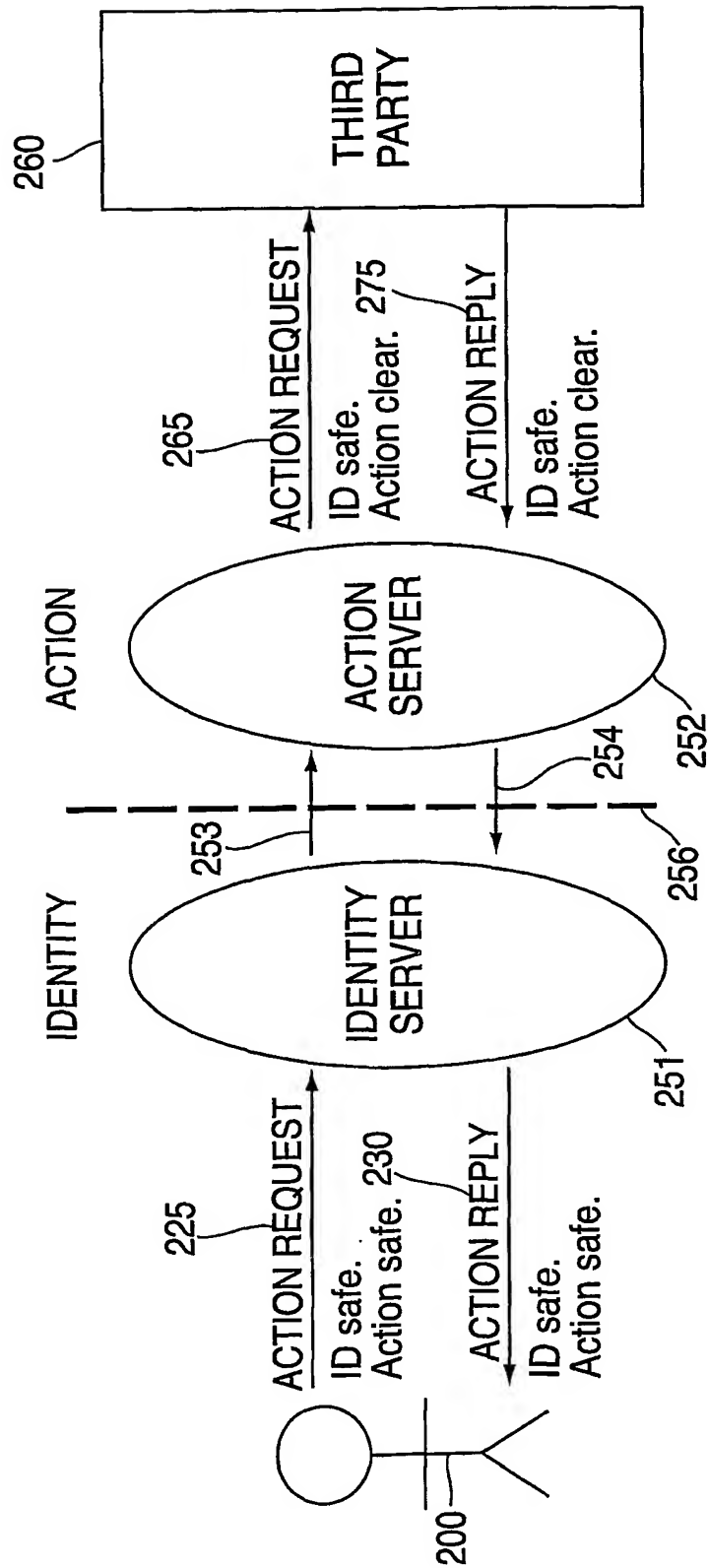


FIG. 2

4/22

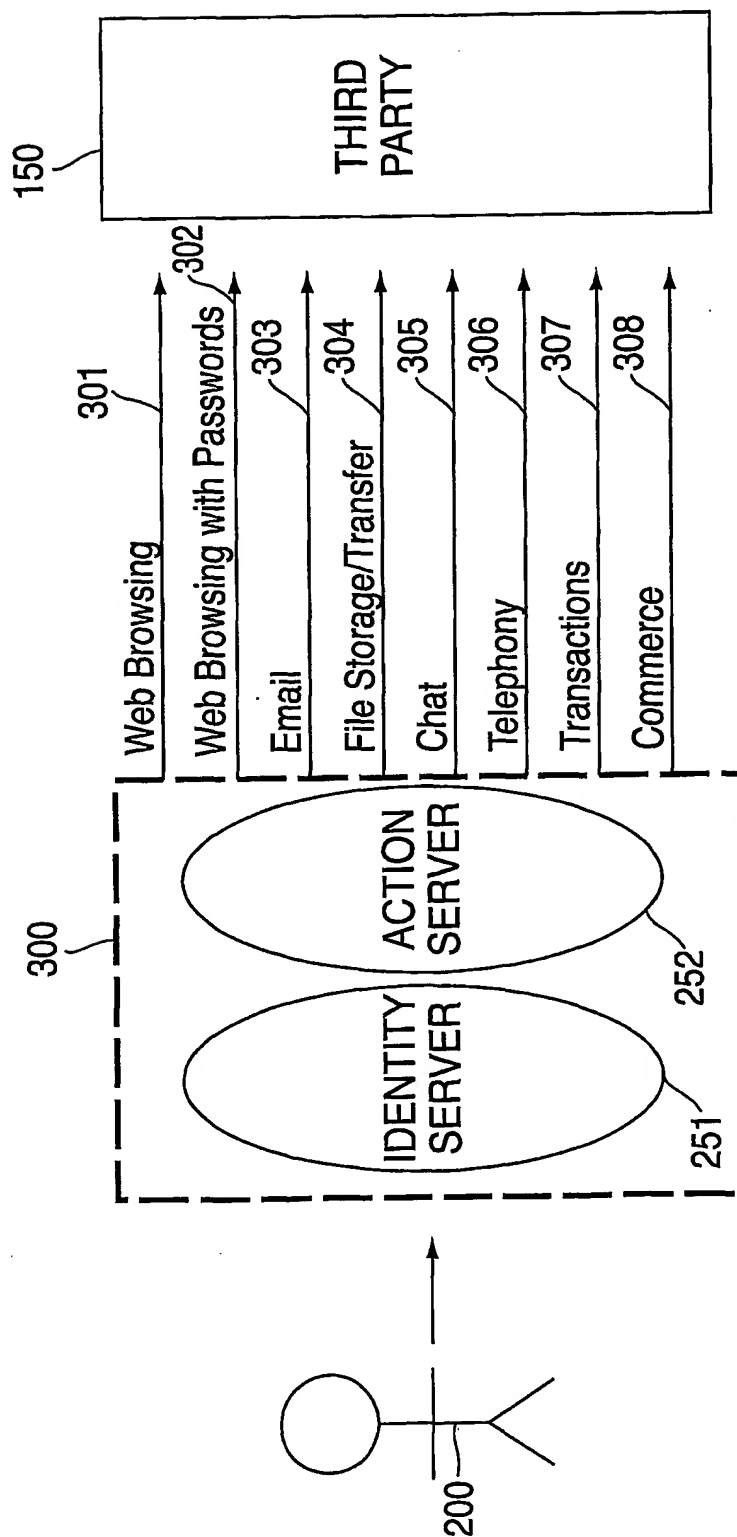


FIG. 3

5/22

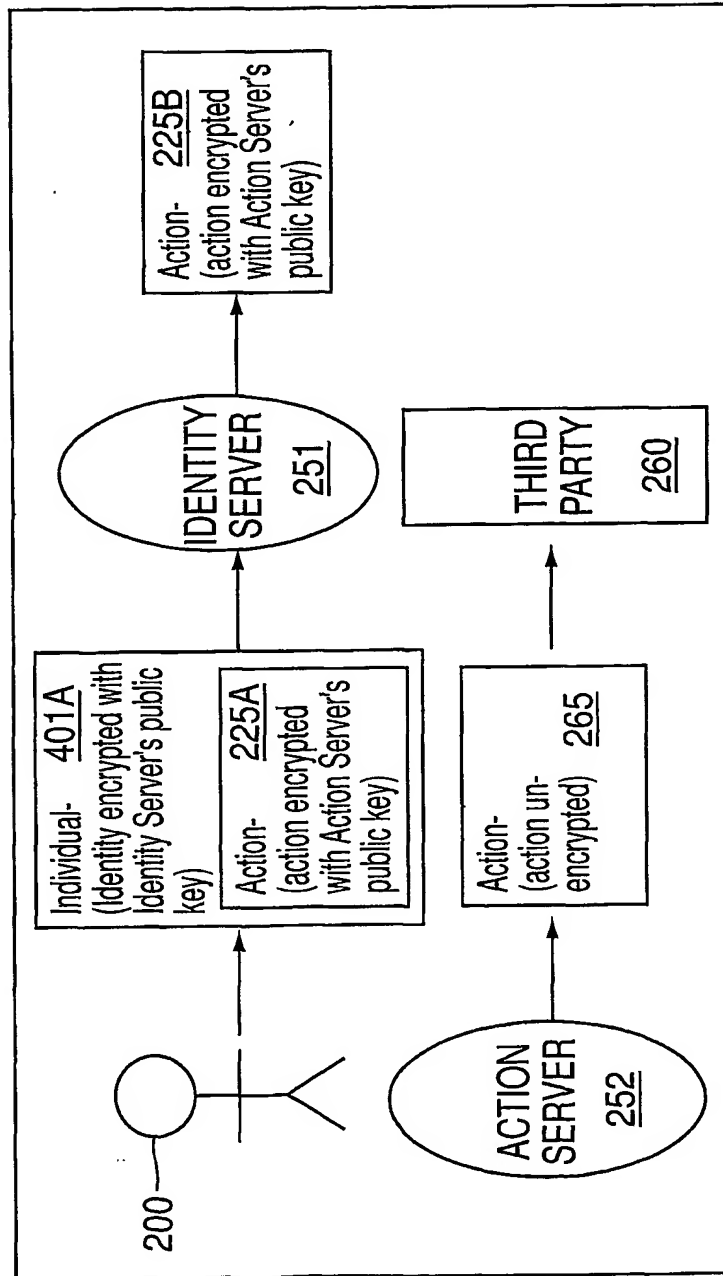


FIG. 4

6/22

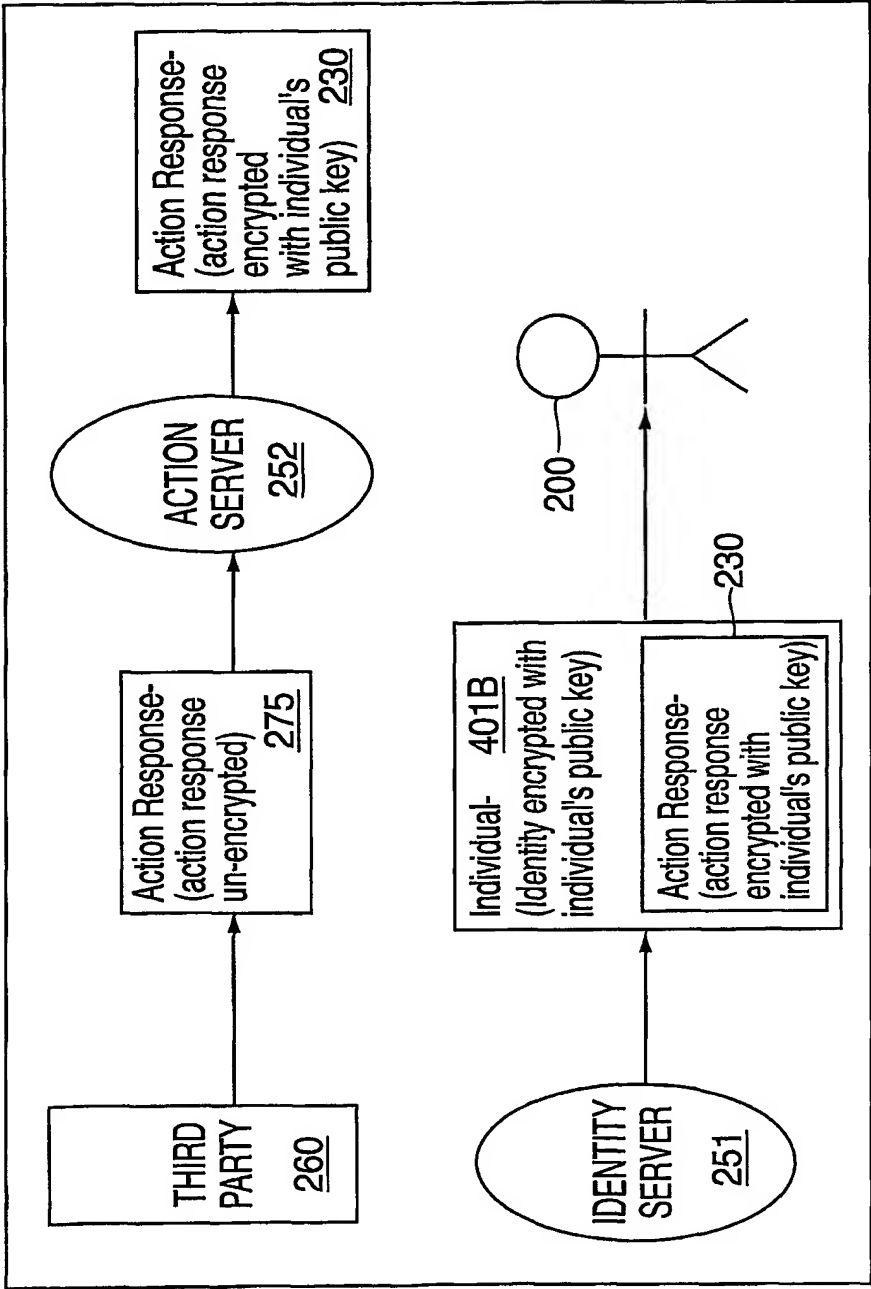


FIG. 5

7/22

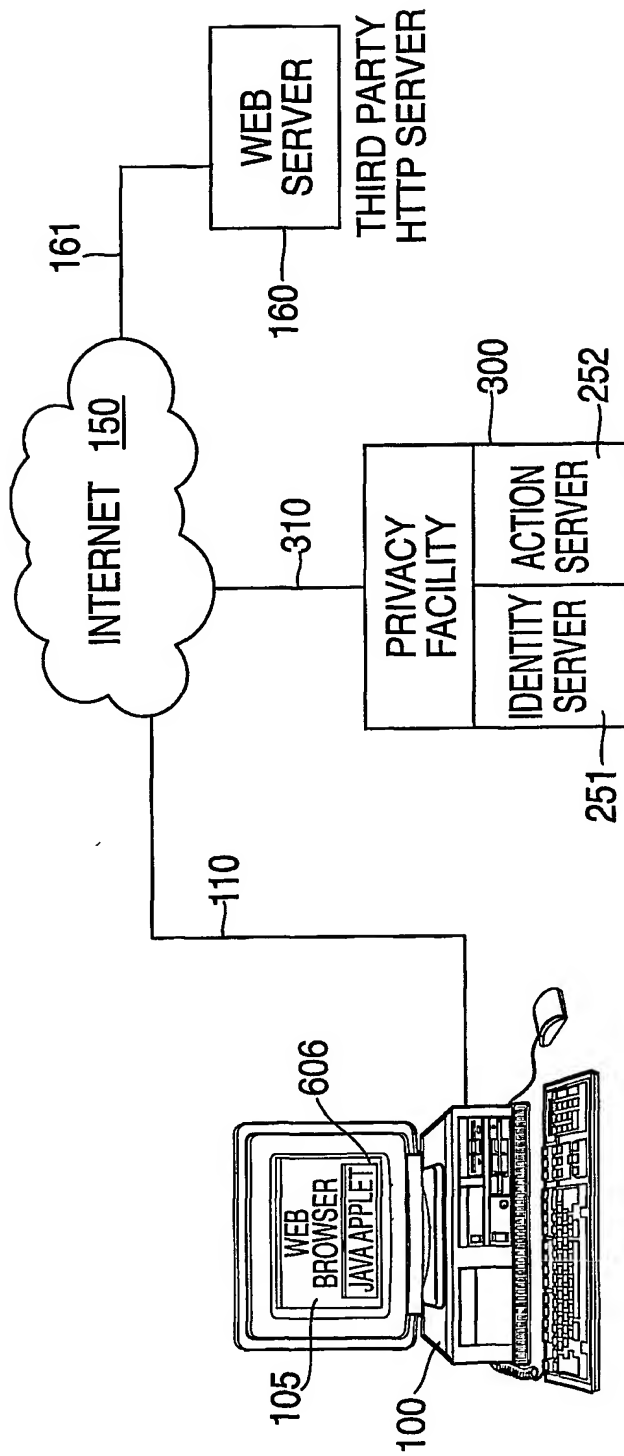


FIG. 6

8/22

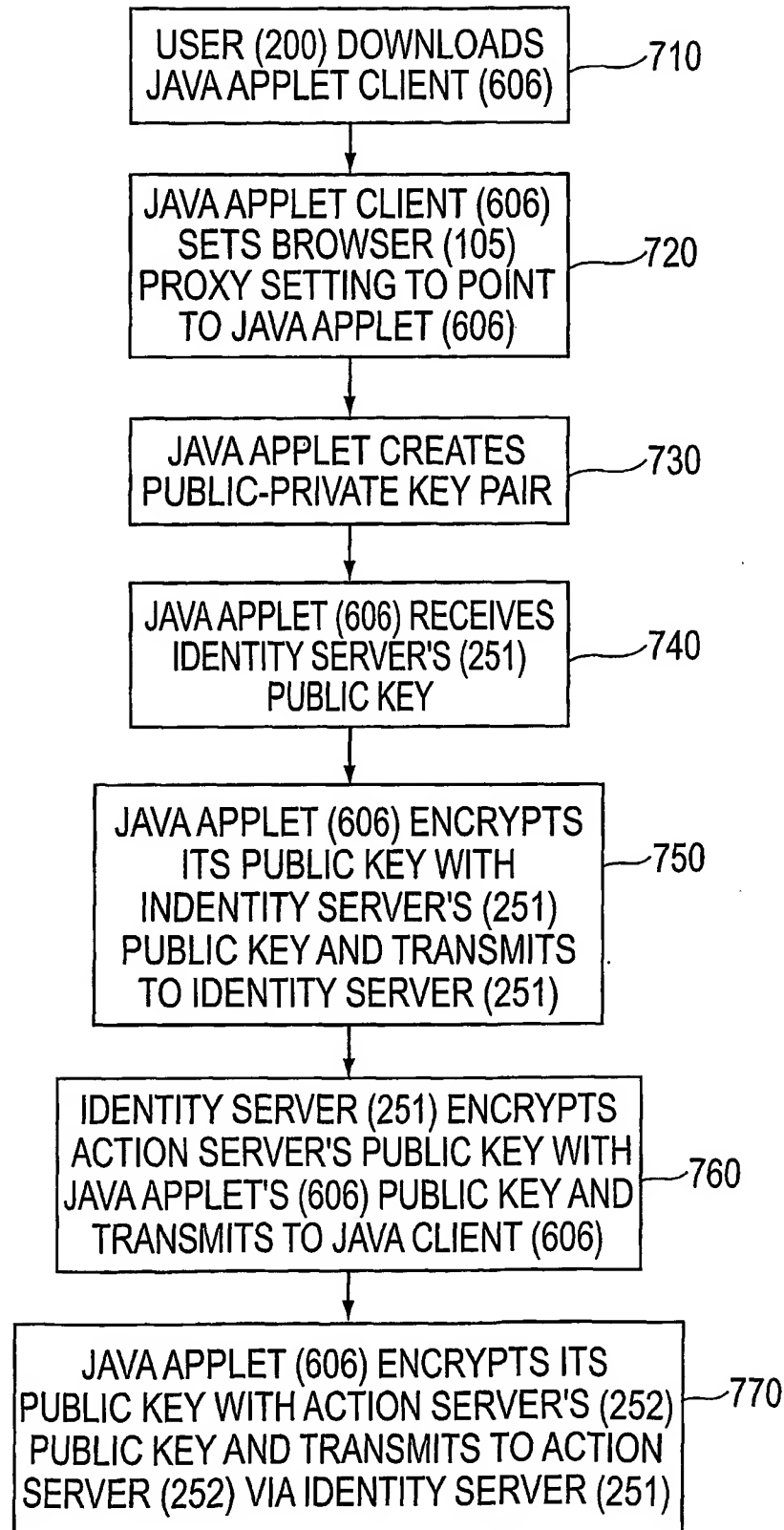


FIG. 7
SESSION INITIALIZATION

9/22

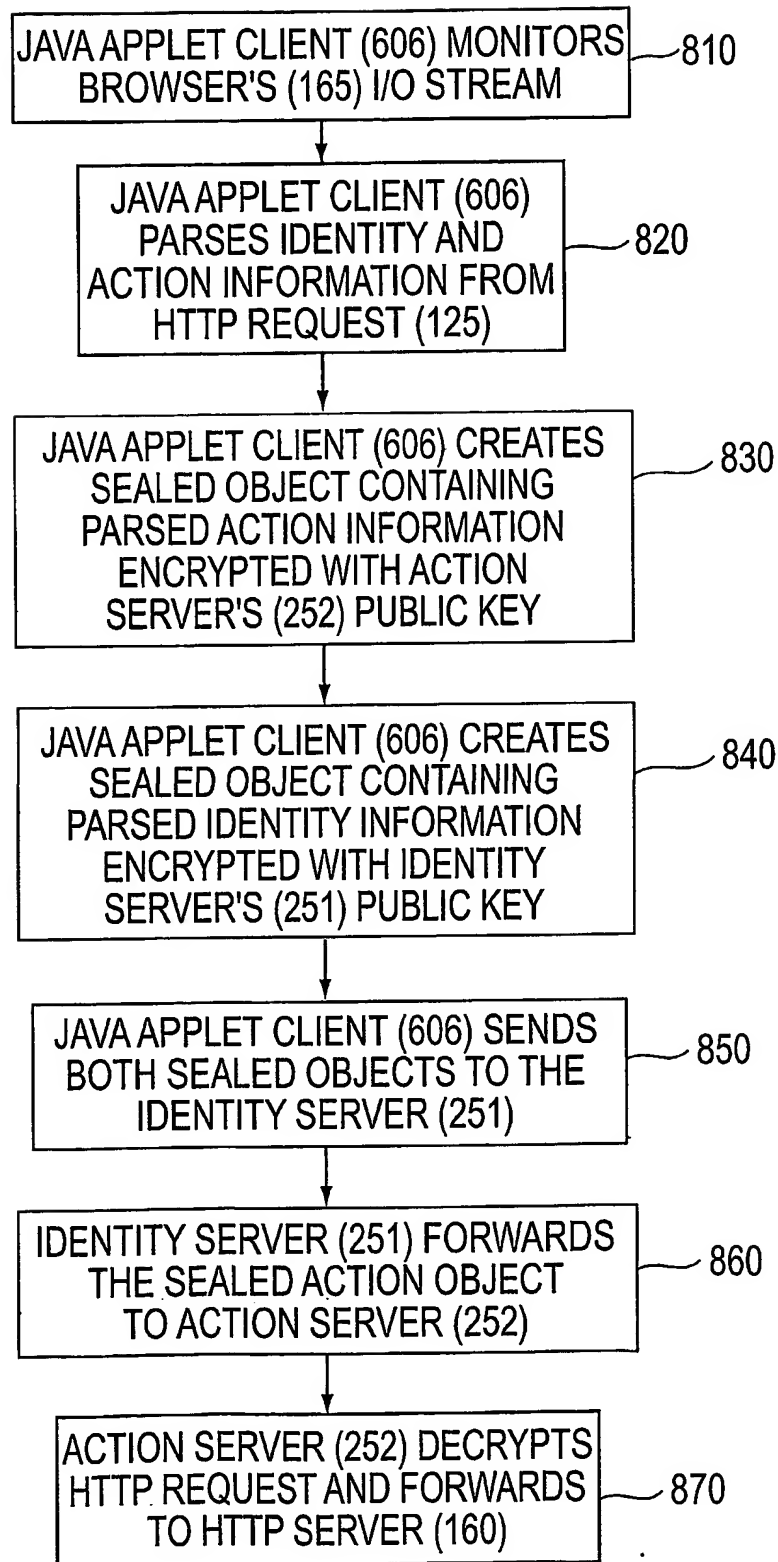


FIG. 8
REQUEST TRANSMISSION

10/22

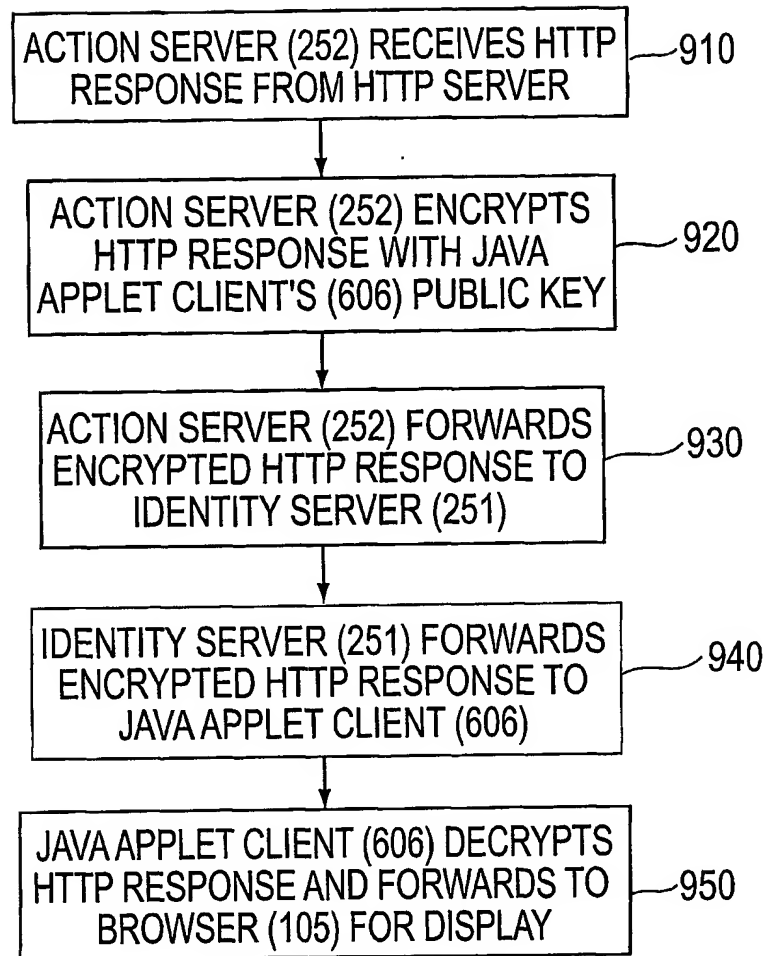


FIG. 9
RESPONSE TRANSMISSION

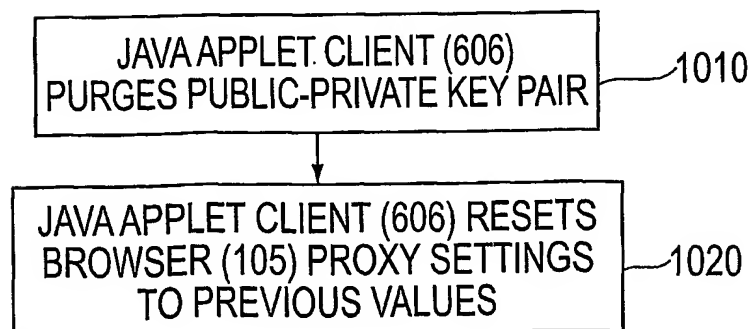


FIG. 10
SESSION TERMINATION

11/22

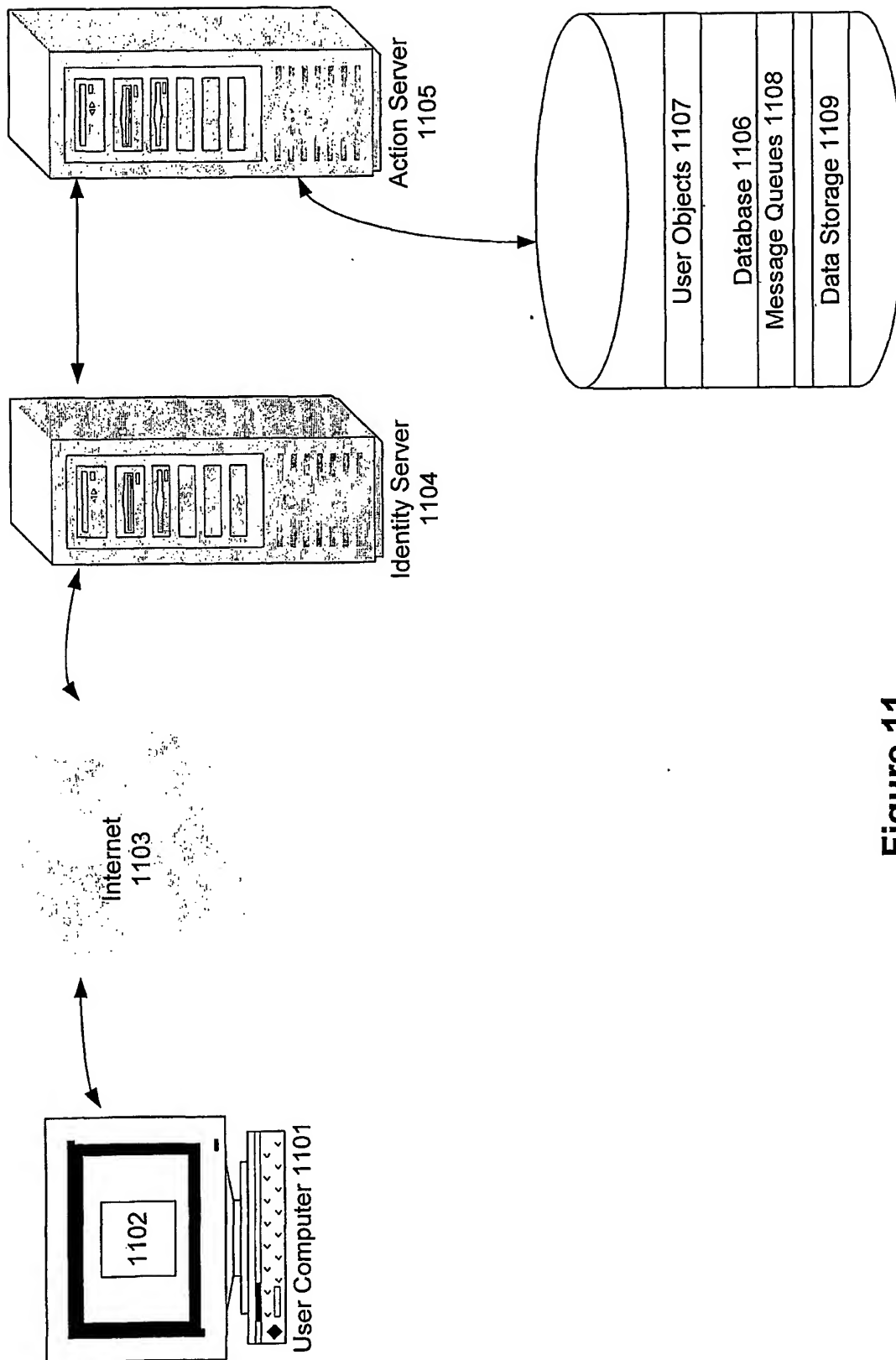


Figure 11

Logical Data Model

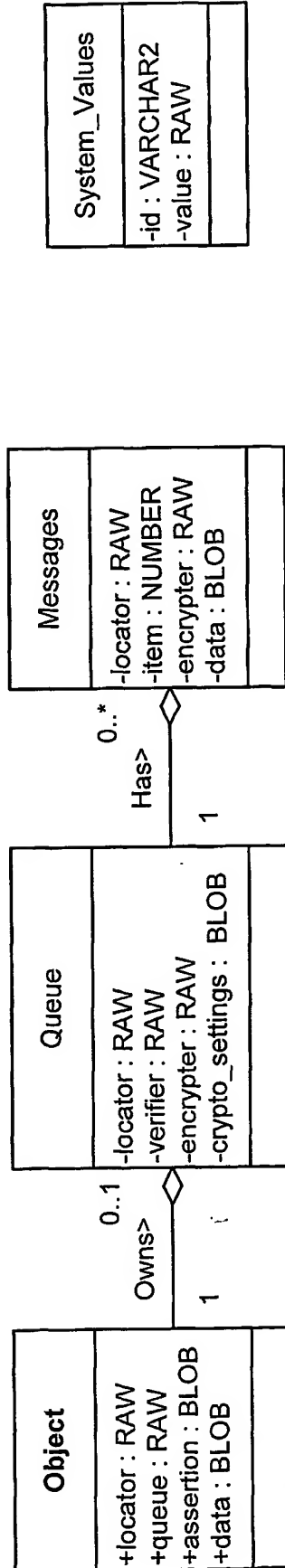


Figure 12

12/22

System_Values
-id : VARCHAR2
-value : RAW

13/22

Client Data Objects

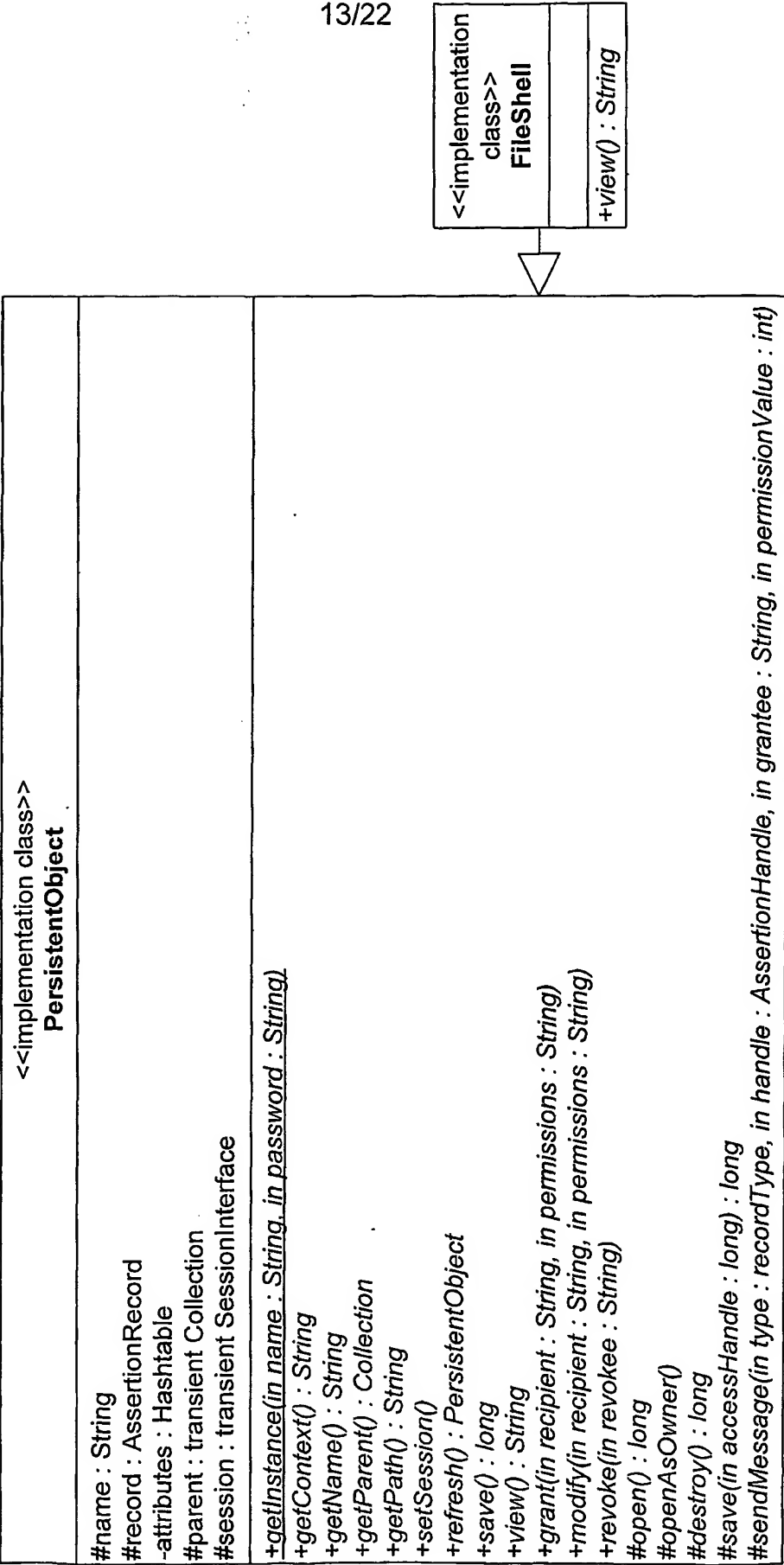


Figure 13

14/22

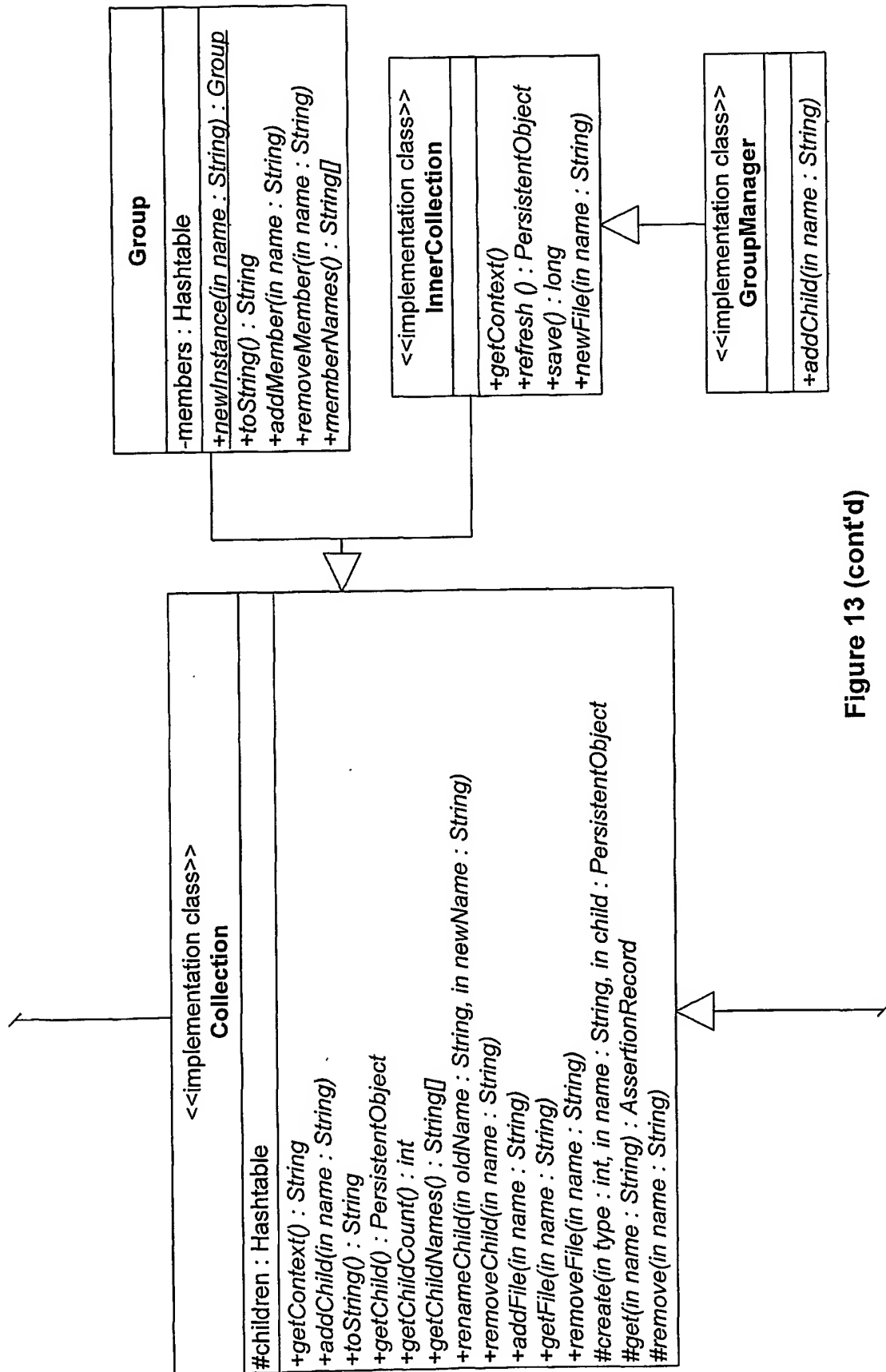


Figure 13 (cont'd)

15/22

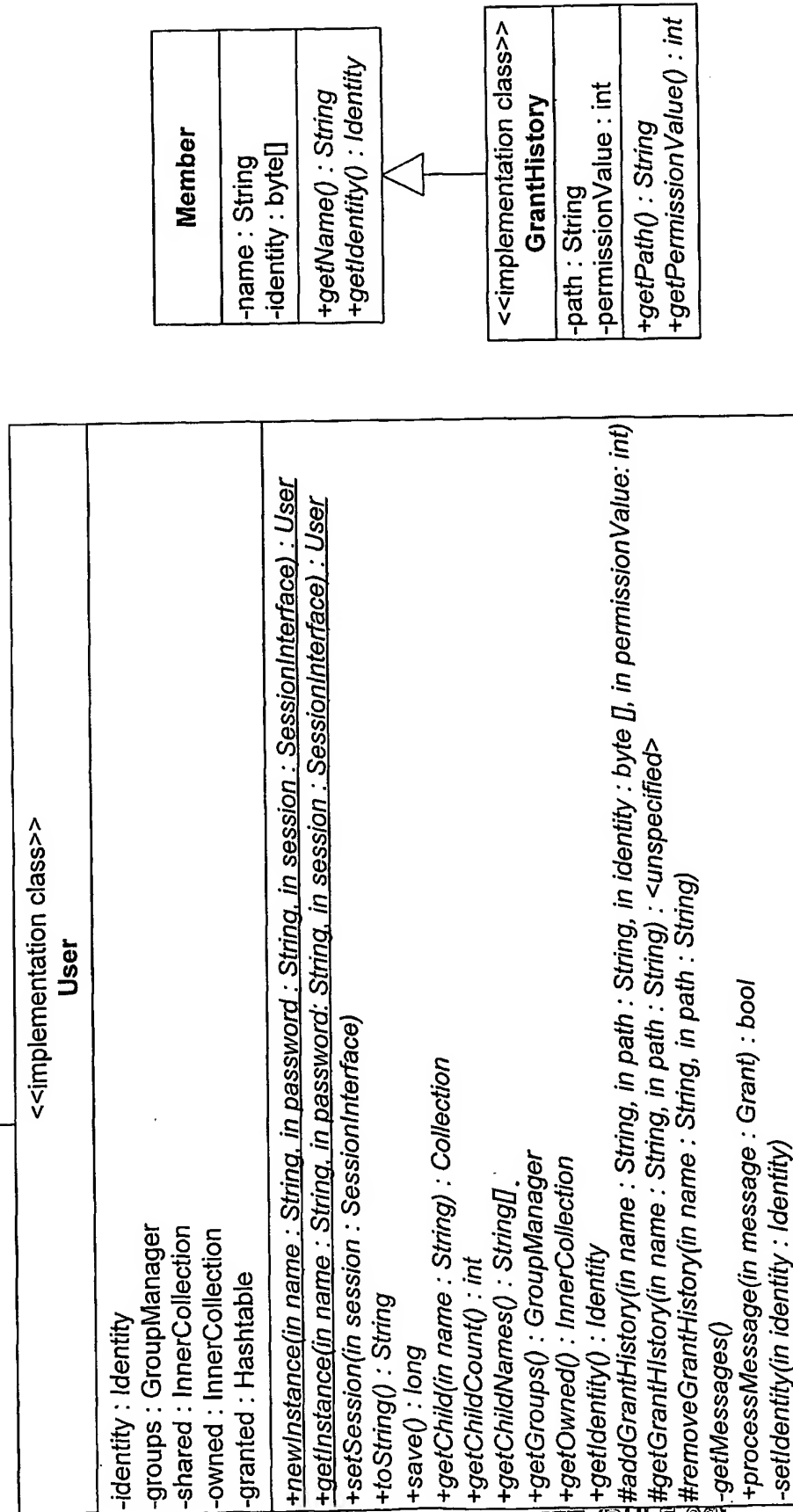


Figure 13 (cont'd)

Client Data Record Objects

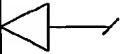
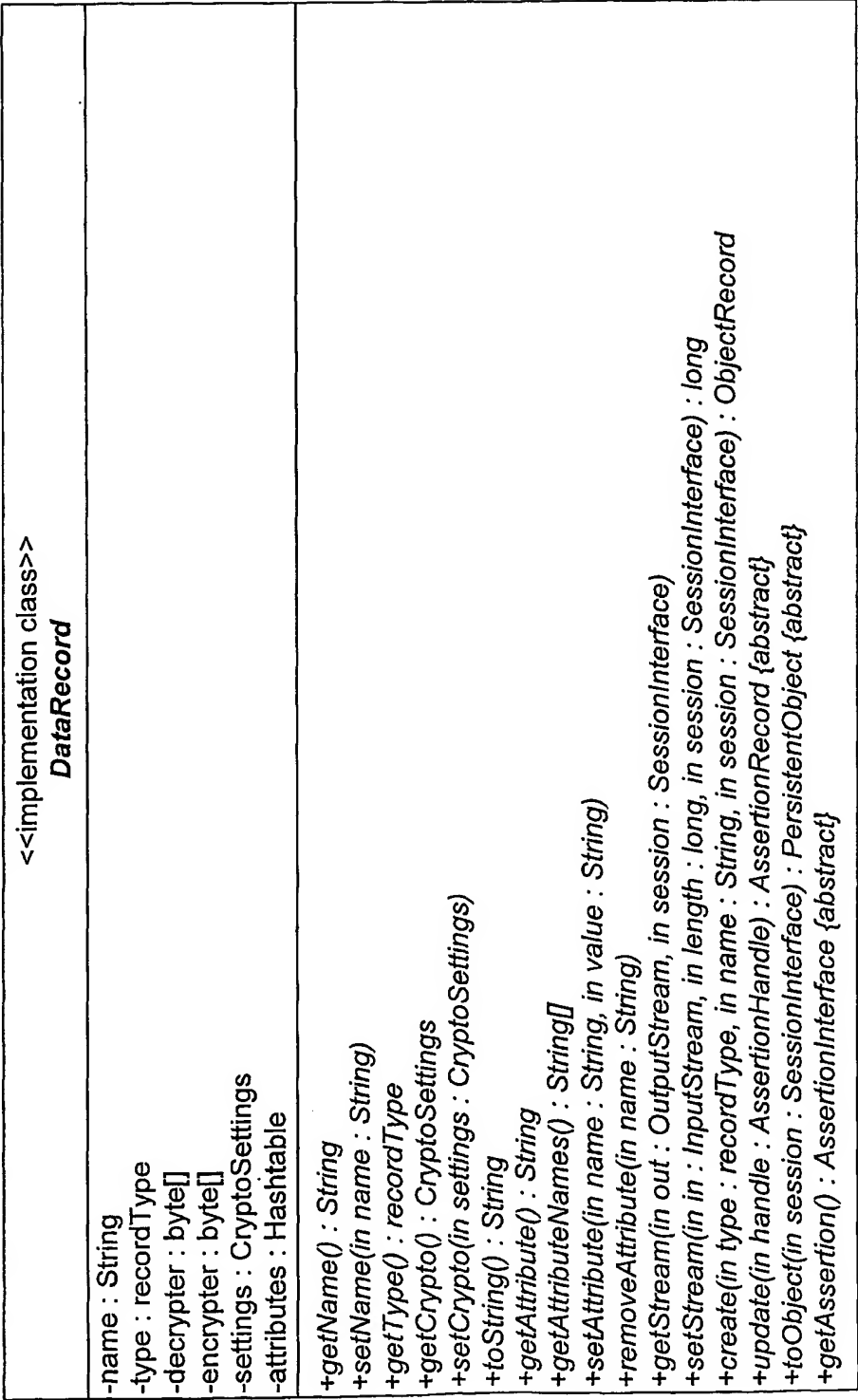


Figure 14

17/22

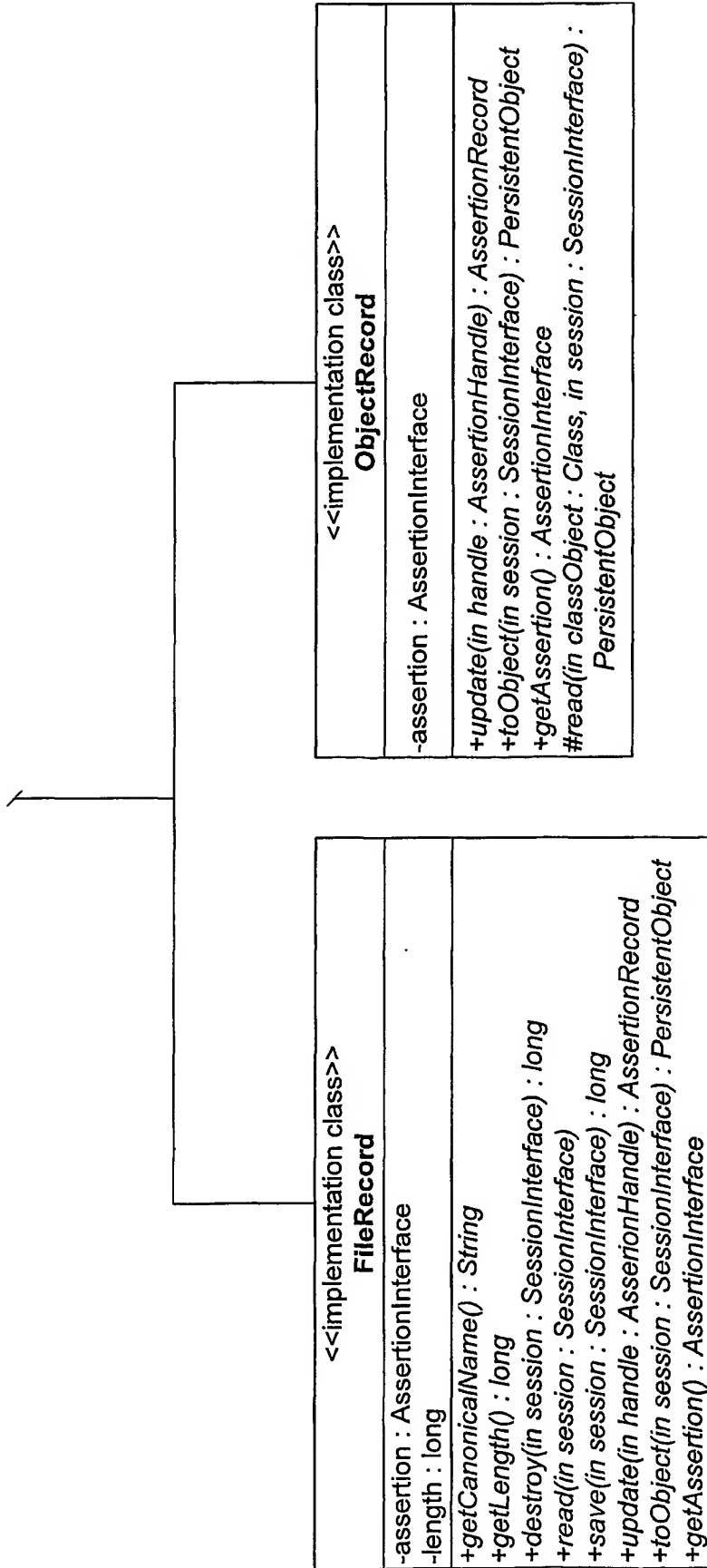


Figure 14 (cont'd)

<<implementation class>> Identity	
-queueIdentifier : byte[] -messageDecrypter : byte[] -ownerIdentifier : byte[] -ownerVerifier : byte[] -crypto : transient AsymmetricCryptoPackage	
+getOwnerVerifier() : byte[] +assertOwnership(in cryptography : CryptoManager, in handle : ChallengeHandle) : Challenge +assertAuthorship(in cryptography : CryptoManager, in handle : ChallengeHandle) : Challenge +assertMembership(in cryptography : CryptoManager, in handle : ChallengeHandle, in identity : byte[]) : Challenge +decryptMessage(in cryptography : CryptoManager, in messageKey : byte[], in settings : CryptoSettings, in messageBody : byte[]) : byte[]	

18/22

<<enumeration>> recordType

<<implementation class>> Grant
-type : recordType -grantor : String -description : String -permissionValue : int +getType() : recordType +getGrantor() : String +getDescription() : String +getPermissionValue() : int +toString() : String

Figure 14 (cont'd)

19/22

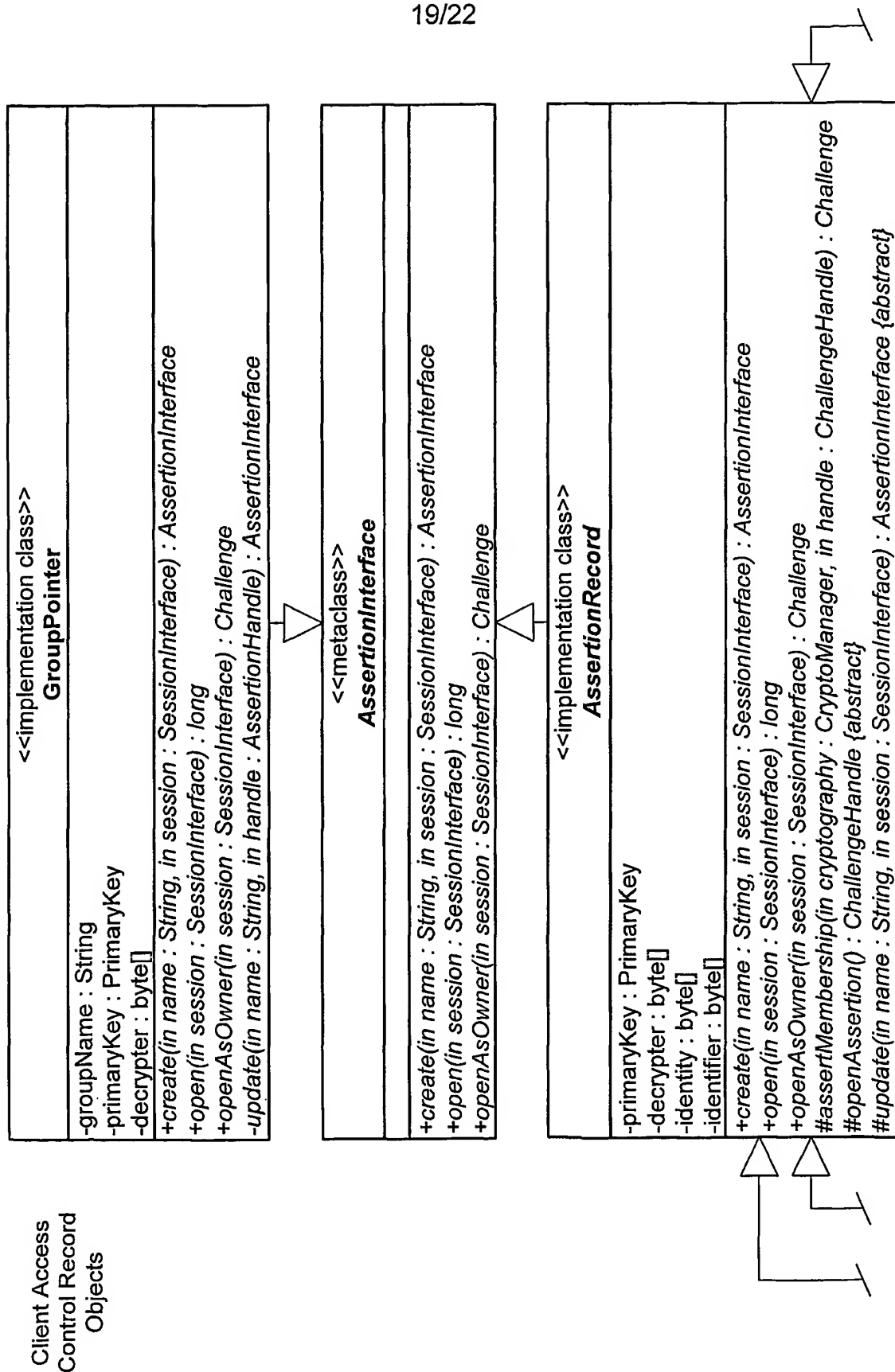


Figure 15

20/22

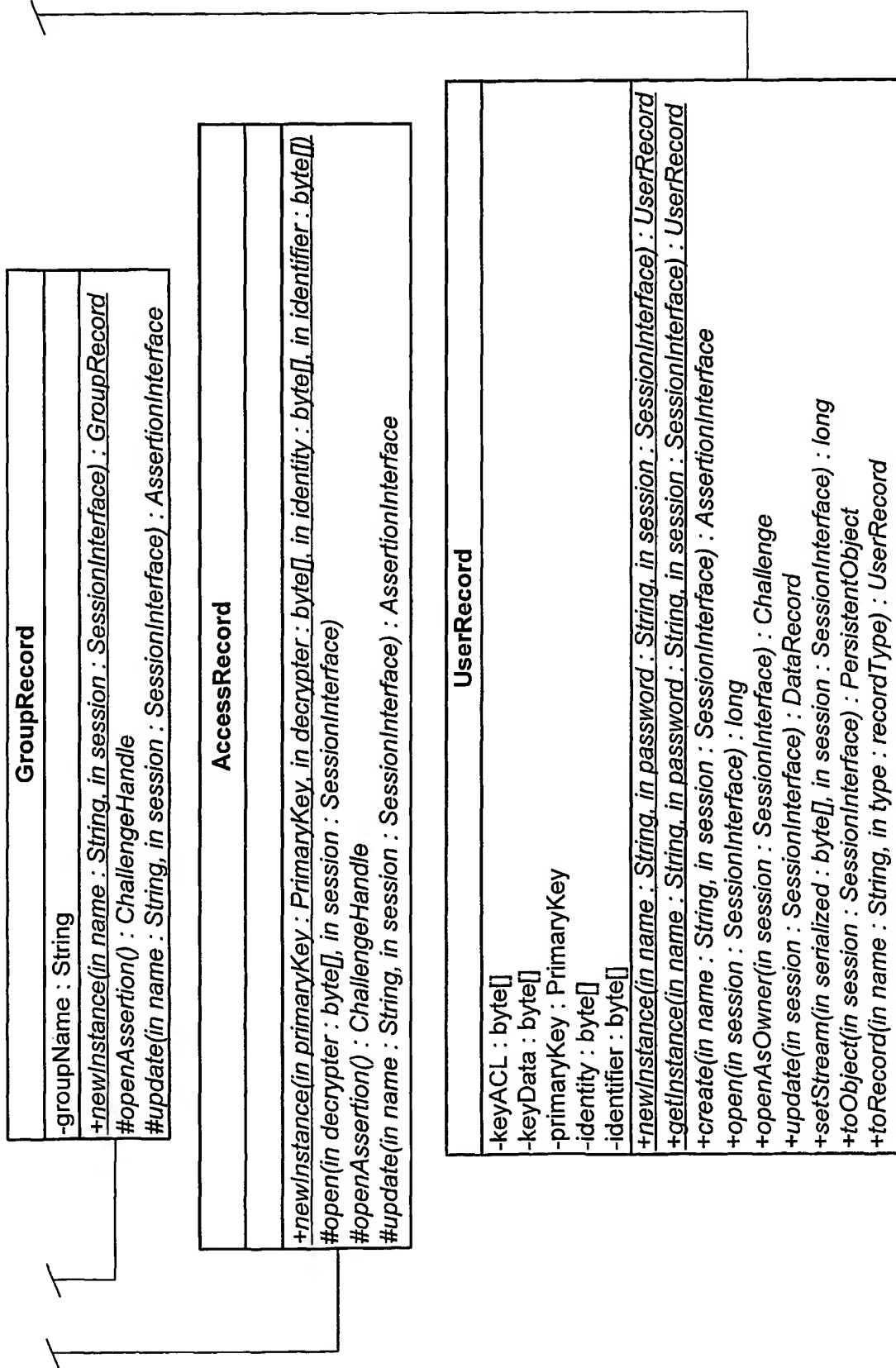


Figure 15 (Cont'd)

Server Access Control Objects

<<implementation class>> AccessControlList	<pre> +newInstance(in client : DatabaseClient, in primaryKey : PrimaryKey, in encrypter : byte[], in ownerVerifier : byte[], in identity : byte[], in verifier : byte[], in permissionValue : int) : AccessControlList +newInstance(in client : DatabaseClient, in primaryKey : PrimaryKey, in encrypter : byte[], in parent : Group, in groupIdentity : byte[], in groupVerifier : byte[]) : AccessControlList +newInstance(in client : DatabaseClient, in parent : AccessControlList, in primaryKey : PrimaryKey, in encrypter : byte[]) : AccessControlList +getInstance(in client : DatabaseClient, in primaryKey : PrimaryKey, in decrypter : byte[]) : AccessControlList +assert(in permissionType : int, in identity : byte[]) : int +addEntry(in identity : byte[], in verifier : byte[], in permissionValue : int) +setEntry(in identity : byte[], in verifier : byte[], in permissionValue : int) +removeEntry(in identity : byte[], in verifier : byte[]) -checkPermissions(in permissionType : int, in identity : byte[]) : int </pre>
<<implementation class>> Group	<pre> -accessIdentity : byte[] -accessVerifier : byte[] +newInstance(in client : DatabaseClient, in pk : PrimaryKey, in encrypter : byte[], in ownerVerifier : byte[], in accessIdentity : byte[], in accessVerifier : byte[], in identity : byte[], in verifier : byte[]) : Group +getInstance(in client : DatabaseClient, in primaryKey : PrimaryKey, in decrypter : byte[]) : Group +getAccessIdentity() : byte[] +getAccessVerifier() : byte[] +destroy() +addMember(in identity : byte[], in verifier : byte[]) +removeMember(in identity : byte[]) </pre>

Figure 16

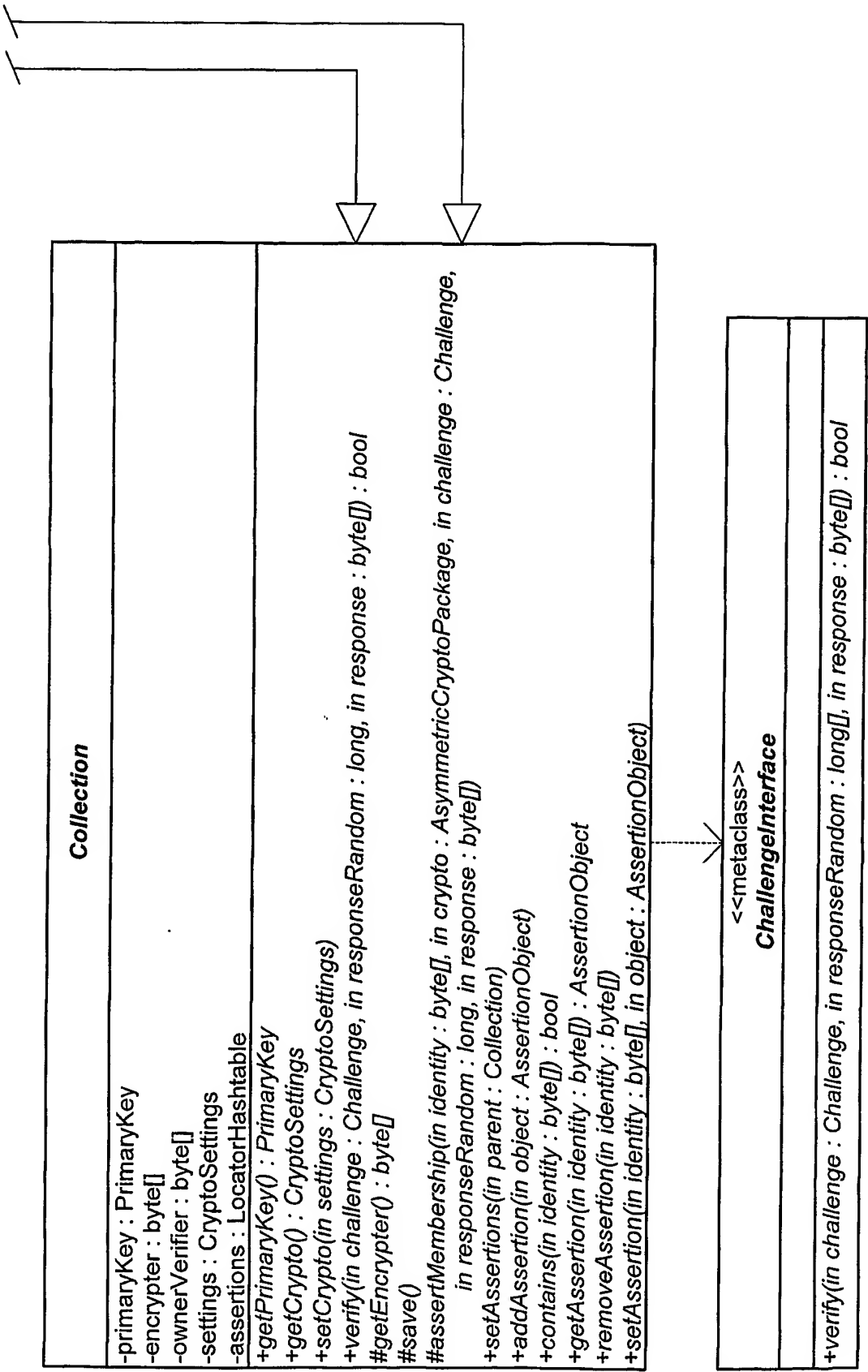


Figure 16 (cont'd)